UNITED STATES PATENT APPLICATION

FOR

**Reducing Problems Caused By Variations In Watermark
Detection Results**

INVENTOR:

Michael S. Ripley

INTEL CORPORATION

Prepared by:

Steven P. Skabrat

Reg. No. 36,279

(503) 264-8074

Express Mail No. <u>EV 325528304 US</u>

Reducing Problems Caused By Variations In Watermark Detection Results

5

BACKGROUND

1. FIELD

10   The present invention relates generally to content protection and security in computer and consumer electronics systems and, more specifically, to watermark detection.

2. DESCRIPTION

15   A number of systems for protecting content (e.g., against unauthorized copying) have been developed that employ watermarking as a part of the protection scheme. Watermarking is a technique whereby information is embedded into content in such a way that is generally transparent to users of the content, is difficult to remove from the content, and can be robustly detected in 20 the content by specialized hardware or software. In some systems, the watermark data may indicate conditions and requirements constraining use of the content, including constraints specific to copying, with the intent that such information is robustly carried with the content when in an analog or unencrypted digital form. A recording device that is compliant with such a system may be 25 required to detect the watermark in unencrypted content that is to be copied. If the watermark is present and indicates that a copy is not permitted, then the recording device does not make a copy. If the watermark is present and indicates that a copy is permitted, the recording device may be required to apply cryptographic protection (i.e., encryption) to any authorized copy of that content 30 made by the recording device. In that case, compliant player devices may be required to detect the watermark in unencrypted recordings that are to be played, and stop playback if the watermark is detected (since such content either should

not have been recorded, or should have been recorded in a cryptographically protected manner).

Unfortunately, real world properties of watermark technologies lead to challenging practical problems when watermarks are used in such a manner.

5

BRIEF DESCRIPTION OF THE DRAWINGS

The features and advantages of the present invention will become
10   apparent from the following detailed description of the present invention in which:

Figure 1 is a diagram of known system using watermarks; and

Figure 2 is a diagram illustrating a system using watermarks according to an embodiment of the present invention.

15

DETAILED DESCRIPTION

An embodiment of the present invention is a system for overcoming
20   practical problems in implementing watermark detection in recording and playback devices. In embodiments of the present invention, the sensitivities of a watermark detection component of a compliant recording device and a compliant playback device may be adjusted so as to reduce the likelihood of playback problems.

25   Reference in the specification to "one embodiment" or "an embodiment" of the present invention means that a particular feature, structure or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, the appearances of the phrase "in one embodiment" appearing in various places throughout the specification are
30   not necessarily all referring to the same embodiment.

One class of practical problems using watermarks in consumer electronics devices or computer systems can arise where detection of the watermark is non-deterministic or otherwise varies from one content protection implementation to another. Non-deterministic, as used herein, means that the content processed

5 by one device might produce different results each time the content is processed, or that the content processed by one device produces different results than the same content processed by another device. For example, some schemes may call for watermark screening to occur at random intervals. In such cases, a given piece of content may be found by one content protection

10 implementation to contain a watermark, and by another implementation (or that same implementation at a later time) to not contain the watermark. This causes problems if, for example, a recording device fails to detect a watermark and therefore records content in the clear, whereas a playback device detects the watermark in that same content and refuses to play the recording.

15 Inconsistent results in watermark detection may occur for various reasons. For example, in a given watermark detection system, there may be an allowance for variation of the precision of the arithmetic used in the watermark detection component. As a result, inconsistent detection results may computed in different devices if the computational precision of the recording and playback devices is

20 different. In another example of processing content in the form of watermarked multiple channel audio data, in order to save manufacturing costs, a device manufacturer may provide a watermark detection component in a recording device that checks randomly across six channels of audio data or otherwise is less likely to detect a watermark. Another manufacturer of a playback device

25 may provide a different watermark detection component that checks the six channels in another manner or otherwise is more likely to detect the watermark.

Figure 1 is a diagram of a known system using watermarks that illustrates this problem. Content 10 may be unencrypted, with a watermark embedded within the content. When this content is read by a compliant recording device

30 12, a watermark detection component 14 will examine the content to attempt to detect a watermark. If a watermark is detected in the content by watermark

detection component 14, then path 16 is taken and the recording device encrypts the content using encryption component 18 to produce encrypted recording 20. Encrypted recording 20 may then be read by a compliant playback device 22 using a decryption component 23 and a player component 24. The compliant playback device recognizes that the content is encrypted, and this takes precedence over checking for a watermark in the content. The player component decrypts the encrypted recording and renders the content for perception by a user.

If a watermark is not detected in the content by watermark detection component 14 of the compliant recording device (although the watermark is actually in the content), then path 26 is taken and the unencrypted content is not encrypted and a recording is made by the compliant recording device as unencrypted recording 28. The failure of the watermark detection component in the compliant recording device to detect the watermark in the content results in an assumption that the content may be redistributed in the clear. When unencrypted recording 28 is read by compliant playback device 22, the playback device recognizes that the content in the unencrypted recording is in the clear, so watermark detection component 30 of the compliant playback device attempts to find a watermark in the unencrypted content. If the watermark is not detected, then the player component 24 renders the unencrypted content. This content, from the point of view of the playback device, may be freely rendered and/or distributed. However, if a watermark is detected in the unencrypted recording by the watermark detection component of the compliant playback device, then the playback device does not render the content (assuming the watermark indicates a prohibition on copying or on playback of an unauthorized copy). Hence, a problem occurs when the compliant recording device does not detect the watermark, but the compliant playback device does.

Embodiments of the present invention address this problem probabilistically by differentiating the watermark detection capabilities associated with the compliant recording device and the compliant playback device. In particular, the watermark detection component in the compliant recording device

5

used for controlling recording of content may be set to be more sensitive to the presence of watermarks, and the watermark detection component in the compliant playback device may be set to be less sensitive to the presence of watermarks. When the watermark detector in the recording device is more

5   sensitive, it is more likely that the recording device will detect the watermark. For example, a recording device's watermark detection component may check for the watermark frequently when processing the unencrypted content, and a playback device's watermark detection component may check for the watermark less frequently. As a result, the likelihood of the problem described above

10   occurring may be reduced, since it will occur only if the more sensitive watermark detector in the recording device misses a watermark and the less sensitive watermark detector in the playback device detects the watermark.

Figure 2 is a diagram illustrating a system using watermarks according to an embodiment of the present invention. In this embodiment, content 10 may be

15   unencrypted, with a watermark embedded within the content as before. When this content is read by a compliant recording device 36, a new more sensitive watermark detection component 38 will examine the content to attempt to detect a watermark. If a watermark is detected in the content by sensitive watermark detection component 38, then path 40 is taken and the recording device encrypts

20   the content using encryption component 18 to produce encrypted recording 20. Encrypted recording 20 may then be read by a compliant playback device 42 using a decryption component 23 and a player component 24 as before. The compliant recording device recognizes that the content is encrypted, and this takes precedence over checking for a watermark in the content. The player

25   component decrypts the encrypted recording and renders the content for perception by a user.

If a watermark is not detected in the content by sensitive watermark detection component 38 of the compliant recording device (although the watermark is actually in the content), then path 44 is taken and the unencrypted

30   content is not encrypted and a recording is made by the compliant recording device as unencrypted recording 28. The failure of the watermark detection

component in the compliant recording device to detect the watermark in the content results in an assumption that the content may be redistributed in the clear. However, in embodiments of the present invention, since the watermark detection component 38 is more sensitive than traditional watermark detectors,

5   the likelihood of missing the watermark is lower than before. When unencrypted recording 28 is read by compliant playback device 42, the playback device recognizes that the content in the unencrypted recording is in the clear, so less sensitive watermark detection component 50 of the compliant playback device attempts to find a watermark in the unencrypted content. If the watermark is not

10   detected, then the player component 24 renders the unencrypted content. This content, from the point of view of the playback device, may be freely rendered and/or distributed. This is the likely path since the more sensitive watermark detector in the compliant recording device did not detect a watermark in the content.

15   If a watermark is detected in the unencrypted recording by the less sensitive watermark detection component 50 of the compliant playback device, then the playback device does not render the content. This outcome should be much less likely to occur in embodiments of the present invention than previous systems. Thus, the usability and interoperability of compliant recording and

20   playback devices is increased. There is now a higher threshold for detection of "false positives" by the playback device.

In various embodiments, the sensitivity of the watermark detection components 38, 50 may be adjusted in different ways. For example, when the content is six channel audio data, the watermark detection component in the

25   recording device may check more than one channel, or all channels at a time for the watermark, instead of just one of the channels. In another example, the watermark detection component in the recording device may check for the watermark more often than in previous systems. In yet another example, the tolerance or precision of computation used in watermark detection computations

30   may be adjusted so that a watermark is more likely to be found by the recording device. In one embodiment, the sensitivity of the watermark detection

component in the recording device may be adjusted so that the precision of the watermark detection computation is less than the precision used by the watermark detection component in the playback device. These adjustments are merely illustrative and it is contemplated that any adjustment in watermark

5 detection sensitivity may be used and be within the scope of the present invention.

In one embodiment, the compliant recording device and the compliant playback device are integral.

The techniques described herein are not limited to any particular

10 hardware or software configuration; they may find applicability in any computing or processing environment. The techniques may be implemented in hardware, software, or a combination of the two. The techniques may be implemented in programs executing on programmable machines such as mobile or stationary computers, personal digital assistants, set top boxes, cellular telephones and

15 pagers, consumer electronics devices, and other electronic devices, that each include a processor, a storage medium readable by the processor (including volatile and non-volatile memory and/or storage elements), at least one input device, and one or more output devices. Program code is applied to the data entered using the input device to perform the functions described and to

20 generate output information. The output information may be applied to one or more output devices. One of ordinary skill in the art may appreciate that the invention can be practiced with various computer system configurations, including multiprocessor systems, minicomputers, mainframe computers, consumer electronics devices, and the like. The invention can also be practiced

25 in distributed computing environments where tasks may be performed by remote processing devices that are linked through a communications network.

Each program may be implemented in a high level procedural or object oriented programming language to communicate with a processing system. However, programs may be implemented in assembly or machine language, if

30 desired. In any case, the language may be compiled or interpreted.

8

Program instructions may be used to cause a general-purpose or special-purpose processing system that is programmed with the instructions to perform the operations described herein. Alternatively, the operations may be performed by specific hardware components that contain hardwired logic for performing the

5   operations, or by any combination of programmed computer components and custom hardware components. The methods described herein may be provided as a computer program product that may include a machine readable medium having stored thereon instructions that may be used to program a processing system or other electronic device to perform the methods. The term "machine

10   readable medium" used herein shall include any medium that is capable of storing or encoding a sequence of instructions for execution by the machine and that cause the machine to perform any one of the methods described herein. The term "machine readable medium" shall accordingly include, but not be limited to, solid-state memories, optical and magnetic disks, and a carrier wave

15   that encodes a data signal. Furthermore, it is common in the art to speak of software, in one form or another (e.g., program, procedure, process, application, module, logic, and so on) as taking an action or causing a result. Such expressions are merely a shorthand way of stating the execution of the software by a processing system cause the processor to perform an action of produce a

20   result.

While this invention has been described with reference to illustrative embodiments, this description is not intended to be construed in a limiting sense. Various modifications of the illustrative embodiments, as well as other embodiments of the invention, which are apparent to persons skilled in the art to

25   which the invention pertains are deemed to lie within the spirit and scope of the invention.